



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

이학박사 학위논문

Almost 2-regular quinary quadratic forms

(거의 모든 2-정규 5변수 이차형식)

2017년 2월

서울대학교 대학원

수리과학부

이 인 환

© 2017 Inhwan Lee

All rights reserved.

Abstract

A (positive definite integral) quadratic form is called almost n -regular if it globally represents all but finitely many quadratic forms of rank n that are locally represented up to isometry.

In this thesis, we discuss the finiteness of primitive almost 2-regular quinary quadratic forms up to isometry. We prove that there are finitely many almost 2-regular quinary quadratic forms that represent all integers. We also prove that there are finitely many primitive almost 2-regular quinary quadratic forms having an odd core prime. We discuss the finiteness of primitive almost 2-regular quinary quadratic forms which have 2 as the only core prime.

Key words: quadratic forms, almost n -regular forms, representation, Watson transformation

Student Number: 2009-22893

Contents

Abstract	iii
1 Introduction	1
2 Preliminaries	5
2.1 Quadratic spaces and lattices	5
2.2 Watson transformation	13
2.3 Analytic tools	16
3 Terminal lattices	19
3.1 Core lattices	19
3.2 Finiteness of terminal lattices	22
4 Almost 2-regular quinary lattices	32
4.1 Even universal almost 2-regular quinary \mathbb{Z} -lattices	32
4.2 Finiteness of even almost 2-regular quinary \mathbb{Z} -lattices	36
Abstract (in Korean)	44

Chapter 1

Introduction

For a positive definite (non-classic) integral quadratic form f , we say that f is *n-regular* if it globally represents all (positive definite integral) quadratic forms of rank n that are locally represented. Similarly, f is called *almost n-regular* if it represents all but finitely many quadratic forms up to isometry. Any (almost) 1-regular form is simply called (almost) regular.

The term ‘regular’ was first coined by Dickson in [7], who determined all regular forms of the form $x^2 + ay^2 + bz^2$, where a, b are positive integers. Watson showed in [18] that there exist only finitely many inequivalent ternary regular forms by using arithmetic arguments. He defined the set $E(f)$ of positive integers which are locally represented, but not globally, by a ternary quadratic form f . He showed that the size of $E(f)$ grows as the discriminant of f increases, and hence only finitely many ternary forms up to isometry can be regular.

The problem of finding all primitive regular ternary forms was reignited by Jagy, Kaplansky and Schiemann who provided a list of 913 (inequivalent) regular ternary quadratic forms including 22 candidates. Their proof relies on the complete list of those regular ternary forms with square-free discriminant [18] and the method of descent which is originated by Watson in [20]. This method of descent involves transformations changing a regular ternary form to another one with smaller discriminant and simpler local structure,

CHAPTER 1. INTRODUCTION

which are called the Watson transformations. Recently, Oh [13] proved the regularity of 8 candidates. For the regularity of the remaining 14 candidates, Oliver [15] proved the regularity of them under the assumption that Generalized Riemann Hypothesis is true. However, it is still beyond our reach to prove the regularities of the remaining 14 candidates without any assumptions.

The study of higher-dimensional analogue of regular quadratic forms is pioneered by Earnest in [8]. He showed that there exist only finitely many inequivalent primitive 2-regular quaternary quadratic forms. His proof mainly uses the estimation of character sums to obtain an upper bound of the discriminant of primitive 2-regular quaternary forms. Chan and Oh [5] made a significant improvement in this direction by proving that for any integer $n \geq 2$, there exist only finitely many inequivalent primitive positive definite n -regular quadratic forms of rank $n + 3$. Note that, for any integer $n \geq 6$, there are infinitely many inequivalent primitive 2-regular forms of rank n . For higher rank cases, it is proved by Oh [12] that for any integer $n \geq 27$, every n -regular (even) form is (even, respectively) n -universal. Also, the minimal rank of n -regular forms has an exponential lower bound for n as it increases.

Turning our interest to almost n -regular forms, we refer to Watson [18] again. As stated above, if the size of the set of exceptional integers is fixed, then there are only finitely many inequivalent almost regular primitive ternary quadratic forms. But the analytic method he used in the proof is not computationally effective in bounding the discriminants of those quadratic forms f for which $E(f)$ is bounded by a prescribed constant. Chan and Oh [6] improved this by proving that for any positive integer k , there exists an effective upper bound for the discriminant of almost regular ternary quadratic forms with at most k exceptional integers. They also provided a characterization of almost regular ternary quadratic forms. Recently, Bochnak and Oh [2] proved that if f is an almost regular quaternary form, then f is p -anisotropic for at most one prime p . Moreover, for a prime p , there exists an

CHAPTER 1. INTRODUCTION

almost regular p -anisotropic form f if and only if $p \leq 37$.

For higher rank cases, Chan and Oh [5] proved that if $n \geq 2$, there exist only finitely many inequivalent primitive almost n -regular forms of $n + 2$ variables. This follows directly from their result on the finiteness of n -regular forms of $n + 3$ variables, for an almost $(n + 1)$ -regular form is also n -regular. Then, as Chan and Oh extended Earnest's finiteness results on regular forms of corank 2 to the case of corank 3, one may ask whether there exist only finitely many inequivalent primitive almost n -regular forms of rank $n + 3$. In this thesis, we study the finiteness of inequivalent primitive almost 2-regular quinary quadratic forms. This result is done by joint work with B.-K. Oh.

The discussion in this thesis will be conducted in geometric language of quadratic spaces and lattices rather than quadratic forms. The term “lattice” will always refer to an integral \mathbb{Z} -lattice on a positive definite quadratic space over \mathbb{Q} . Since we want to include non-classic integral quadratic forms in our discussion, we always assume that any \mathbb{Z} -lattice L is an *even primitive* lattice, that is, the norm of L is $2\mathbb{Z}$, unless stated otherwise.

In Chapter 2, we state several definitions and results on quadratic spaces and lattices. The successive minima, which play a central role in our approach, are also defined and some well-known lemmas on them will be stated. The Watson transformation is introduced to define the “terminal” lattice obtained from an even almost n -regular lattice. In the final section, some analytic results which will be used later are stated.

In Chapter 3, we prove that terminal lattices of even almost 2-regular quinary lattices are finite up to isometry. A lattice N is called a *core lattice* of L if the failure of the representation of N by L implies the failure of the representation of infinitely many sublattices of N by L . As the definition indicates, core lattices are crucial to handle almost n -regular lattices. We provide precise forms of some local core lattices of terminal lattices. Note that a terminal lattice L with sufficiently large discriminant always has an even universal quaternary sublattice M . Note that by “The 290-Theorem” of [1], there exist only finitely many even universal quaternary lattices. Our

CHAPTER 1. INTRODUCTION

proof of the finiteness of terminal lattices consists of constructing binary core lattices which are represented by L but not by M . Here, the universality of M is essential, for it guarantees an upper bound of the 4-th successive minimum of L . Also, in the construction of core lattices, results on the estimation of character sums and the distribution of prime numbers in an arithmetic progression are used to give an upper bound of the 5-th successive minimum.

In Chapter 4, we consider the general case. Since any almost 2-regular quinary lattice L is 1-regular, the third successive minimum of L is bounded by an absolute constant. One may easily show that the set of prime divisors of dL is ‘bounded’ from the fact that the number of terminal lattices is finite up to isometry. Hence, to show the finiteness of almost 2-regular quinary lattices up to isometry, it suffices to show that $\text{ord}_p(dL)$ is bounded for any prime p dividing dL . First, we show that even universal almost 2-regular quinary lattices are finite up to isometry. Next, we show that for any odd prime p , $\text{ord}_p(dL)$ is bounded. Here, the Hilbert Reciprocity Law is used to find an exceptional integer which is represented by L but not by its ternary section. Finally, we consider the case when $p = 2$. Since the third minimum of L is bounded, after taking finite number of Watson transformations to L , we may assume that

$$\begin{cases} \mathbb{H} \rightarrow L_q \text{ for any odd prime } q, \\ L_2 \simeq \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp \langle 4\epsilon \rangle \perp K_2 \end{cases}$$

for some binary \mathbb{Z}_2 -lattice K_2 such that $\mathfrak{s}K_2 \subseteq 8\mathbb{Z}_2$. Under these assumptions, we provide all possible candidates of ternary sections of L . If we show that there does not exist an almost 2-regular quinary lattice under the assumption that $\text{ord}_2(\mathfrak{s}(K_2))$ is sufficiently large, then there are only finitely many primitive almost 2-regular quinary lattices up to isometry.

Chapter 2

Preliminaries

In this chapter, we introduce some definitions and well-known results which will be used in this thesis. In the first section, we review some basic facts and well-known results on quadratic spaces and lattices. Also, the notion of successive minima and their basic properties are introduced. In section 2, we define the Watson transformation and use it to define a terminal lattice. In the final section, we gather some analytic results which are frequently used in the following chapter.

2.1 Quadratic spaces and lattices

A *quadratic space* V over a field F is a finite dimensional vector space over F equipped with a symmetric bilinear form

$$B : V \times V \rightarrow F.$$

Here, B is called *symmetric bilinear* if it satisfies

$$B(x, y) = B(y, x), \quad B(ax + by, z) = aB(x, z) + bB(y, z)$$

CHAPTER 2. PRELIMINARIES

for all $x, y, z \in V$ and for all $a, b \in F$. We use the notation (V, B) to denote a quadratic space V equipped with a symmetric bilinear form B . The *quadratic map* Q associated with B is defined by

$$Q(x) = B(x, x)$$

for any $x \in V$.

Let V be a quadratic space with a symmetric bilinear map B of rank n . Suppose that

$$\mathfrak{B} = \{x_1, x_2, \dots, x_n\}$$

is a basis of V . Then the $n \times n$ matrix

$$(B(x_i, x_j))_{1 \leq i, j \leq n}$$

is called the *matrix* of the quadratic space V with respect to \mathfrak{B} . In this case, we use the following notation

$$V \simeq (B(x_i, x_j)).$$

If the matrix $(B(x_i, x_j))$ is diagonal, then we write

$$V \simeq \langle B(x_1, x_1), \dots, B(x_n, x_n) \rangle.$$

The *discriminant* of V is defined by

$$dV = \det(B(x_i, x_j)) \in (F^*/(F^*)^2) \cup \{0\}.$$

Here, F^* is the group of non-zero elements in F . Note that the discriminant of V is independent of the choice of \mathfrak{B} . If $dV \neq 0$, we say that V is a regular quadratic space.

Let (V, B) and (W, C) be quadratic spaces over a field F . We say that V

CHAPTER 2. PRELIMINARIES

is *represented* by W if there exists a linear map $\sigma : V \rightarrow W$ such that

$$B(x, y) = C(\sigma x, \sigma y)$$

for all elements $x, y \in V$. The map σ is called a *representation* of V in W . Further, if σ is a linear isomorphism, then we say that V and W are *isometric* and denote by $V \simeq W$. In this case, we call σ an *isometry*.

To describe an equivalent condition for a quadratic space (V, B) over \mathbb{Q} to be isometric to another space (W, C) , we introduce the Hilbert symbol and the Hasse symbol.

Definition. Let F be a field one of the p -adic number field \mathbb{Q}_p or the real field \mathbb{R} ($= \mathbb{Q}_\infty$).

- (1) For two elements $\alpha, \beta \in F$, the *Hilbert symbol*

$$\left(\frac{\alpha, \beta}{p} \right)$$

is defined to be 1 if $\alpha x^2 + \beta y^2 = 1$ has a solution $x, y \in F$; otherwise the symbol is defined to be -1 .

- (2) Let V be a regular n -ary quadratic space over F . If V has a splitting

$$V \simeq \langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle,$$

the *Hasse symbol* of V is defined by

$$S_p(V) = \prod_{1 \leq i \leq n} \left(\frac{\alpha_i, d_i}{p} \right),$$

where $d_i = \alpha_1 \cdots \alpha_i$.

The following theorem is often called the Hasse-Minkowski theorem, which gives the exact conditions for two quadratic spaces to be isometric.

CHAPTER 2. PRELIMINARIES

Theorem 2.1. (1) *Two regular quadratic spaces V and W over \mathbb{Q}_p are isometric if and only if*

$$\dim(V) = \dim(W), \quad dV = dW, \quad S_p(V) = S_p(W).$$

(2) *Two regular quadratic spaces V and W over \mathbb{Q} are isometric if and only if V_p and W_p are isometric over \mathbb{Q}_p for all finite and infinite prime numbers p . Here, $V_p = V \otimes \mathbb{Q}_p$.*

Proof. See Theorem 63:20 and Theorem 66:4 in [16]. □

The following theorem says that an important equality holds among Hasse symbols over \mathbb{Q}_p .

Theorem 2.2 (Hilbert Reciprocity Law). *Let V be a quadratic space over \mathbb{Q} and let \mathbf{P} be the set of all finite prime numbers in \mathbb{Z} . Then the following equality holds:*

$$\prod_{p \in \mathbf{P} \cup \{\infty\}} S_p(V) = 1.$$

Proof. See Theorem 71:18 in [16]. □

Let R be a ring one of the rational integer ring \mathbb{Z} or the p -adic integer ring \mathbb{Z}_p . Suppose that F is the quotient field of R . An R -lattice L on a quadratic space (V, B) over F is a finitely generated free R -module such that $FL = V$. Note that L inherits the bilinear map B of V satisfying

$$B : L \times L \rightarrow R$$

and the quadratic map $Q : L \rightarrow R$. We call a lattice L *binary*, *ternary*, *quaternary*, *quinary* and *n -ary*, according as the rank of L is 2, 3, 4, 5 and n , respectively. Let L be an R -lattice of rank n and let

$$\mathfrak{B} = \{x_1, x_2, \dots, x_n\}$$

CHAPTER 2. PRELIMINARIES

be an integral basis of L . As above, the $n \times n$ matrix

$$(B(x_i, x_j))_{1 \leq i, j \leq n}$$

is called the *matrix* of L with respect to \mathfrak{B} . We denote $L \simeq (B(x_i, x_j))$. If the matrix $(B(x_i, x_j))$ is diagonal, then we write

$$L \simeq \langle B(x_1, x_1), \dots, B(x_n, x_n) \rangle.$$

The *discriminant* of L is defined by

$$dL = \det(B(x_i, x_j)) \in R.$$

An R -lattice L is called *isotropic* if there is a non-zero vector $x \in L$ with $Q(x) = 0$; otherwise L is called *anisotropic*. A submodule N of L is called a *sublattice* if N itself is a lattice. For sublattices M, N of L , if $B(x, y) = 0$ for all $x \in M, y \in N$, we write

$$M \perp N.$$

Also, we define the *orthogonal complement* M^\perp of M in L as

$$M^\perp = \{x \in L \mid B(x, y) = 0 \text{ for all } y \in M\}.$$

Note that $M \perp M^\perp$ is a sublattice of L of finite index, and hence

$$dM \cdot dM^\perp = dL \cdot \alpha^2,$$

where $\alpha = [L : M \perp M^\perp]$. Furthermore, dM^\perp divides $dM \cdot dL$ by Proposition 5.3.3 in [10].

We say that an R -lattice M is *represented* by another R -lattice L if there exists a representation $\sigma : FM \rightarrow FL$ such that $\sigma M \subseteq L$. An R -lattice L is called *n -universal* if L represents all R -lattices of rank n . When the field F

CHAPTER 2. PRELIMINARIES

is a global field, the *genus* of L , denoted by $\text{gen}(L)$, is defined by the set of all lattices M in the quadratic space FL such that

$$L_p \simeq M_p \quad \text{for all finite and infinite primes } p \text{ of } F.$$

Here, L_p is the lattice $L \otimes R_p$.

The following theorem says that we can choose a global basis of L which is sufficiently close to a fixed local basis of L_p for a prime number p .

Theorem 2.3. *Let p be a prime number and let $\mathbf{c}_1^p, \mathbf{c}_2^p, \dots, \mathbf{c}_n^p$ be a basis of \mathbb{Z}_p^n with*

$$\det(\mathbf{c}_1^p, \mathbf{c}_2^p, \dots, \mathbf{c}_n^p) = 1.$$

Then, for any $\epsilon > 0$, there is a basis $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_n$ of \mathbb{Z}^n with

$$\det(\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_n) = 1$$

such that

$$\|\mathbf{c}_j - \mathbf{c}_j^p\|_p < \epsilon \quad (1 \leq j \leq n).$$

Here we have used the notation

$$\|\mathbf{b}\|_p = \max |b_j|_p$$

for $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{Q}_p^n$.

Proof. See Theorem 2.1 of Chapter 9 in [3]. □

We define the *scale* of L , denoted by $\mathfrak{s}L$, by the R -module generated by the set

$$B(L, L) = \{B(x, y) \mid x, y \in L\}.$$

The *norm* $\mathfrak{n}L$ of L is defined as the R -module generated by the set $Q(L)$. Note that

$$2\mathfrak{s}L \subseteq \mathfrak{n}L \subseteq \mathfrak{s}L.$$

CHAPTER 2. PRELIMINARIES

We call L *unimodular* if $\mathfrak{s}L = R$ and $dL \in R^\times$. We assume that all \mathbb{Z} -lattices are positive definite and even primitive, that is, the matrices of lattices are positive definite and the norms of lattices are $2\mathbb{Z}$.

The main purpose of this thesis is to study almost n -regular lattices which are defined as below.

Definition. A positive definite \mathbb{Z} -lattice L is called *n -regular* if L represents all \mathbb{Z} -lattices of rank n that are represented by the genus of L . Similarly, we say that L is *almost n -regular* if it represents all but finite lattices that are represented by the genus of L .

Lemma 2.4. *Let L be an almost n -regular \mathbb{Z} -lattice. Then L is $(n - 1)$ -regular.*

Proof. Suppose that a \mathbb{Z} -lattice K of rank $n - 1$ is represented by the genus of L . Then there exists a \mathbb{Z} -lattice M in the genus of L such that $K \subseteq M$ (see 102.5 in [16]). Choose a vector v in the orthogonal complement of K in M . Then the lattice

$$K \perp \mathbb{Z}(av)$$

is represented by $\text{gen}(L)$ for any integer a . Hence, with finite exceptions, $K \perp \mathbb{Z}(av)$ is represented by L . In particular, K is represented by L . \square

We introduce the successive minima of a lattice, which will be used to show the discriminant of a \mathbb{Z} -lattice L is bounded. The following definition is adapted from ([3], Chapter 12).

Definition. Let L be a \mathbb{Z} -lattice of rank n . For $1 \leq j \leq n$, the *j -th successive minimum* of L is the positive integer μ_j such that

1. $\dim(\text{span}\{x \in L \mid Q(x) \leq \mu_j\}) \geq j$, and
2. $\dim(\text{span}\{x \in L \mid Q(x) < \mu_j\}) < j$.

Note that the existence of linearly independent vectors $x_1, \dots, x_n \in L$ with $Q(x_j) = \mu_j$ can be proved by the following lemma.

CHAPTER 2. PRELIMINARIES

Lemma 2.5. *Let L be a \mathbb{Z} -lattice of rank n . For some $j \in \{2, \dots, n\}$, suppose that there exist linearly independent vectors $x_1, \dots, x_{j-1} \in L$ such that $Q(x_i) = \mu_i$ for $i = 1, \dots, j-1$. If $y \in L$ satisfies the inequality $Q(y) < \mu_j$, then*

$$y \in \text{span}\{x_1, \dots, x_{j-1}\} \cap L.$$

Proof. See Lemma 2.2 in [8]. □

For an integer $1 \leq k \leq n$ and vectors $x_1, \dots, x_n \in L$ with $Q(x_i) = \mu_i$, a k -ary section of L is defined as the \mathbb{Z} -lattice

$$\text{span}\{x_1, \dots, x_k\} \cap L.$$

Using Lemma 2.5, one can show that a k -ary section of L gives an upper bound of the $(k+1)$ -th successive minimum of L as follows.

Lemma 2.6. *Let L be a \mathbb{Z} -lattice and M be a k -ary section of L with $k < \text{rank}(L)$. If a binary \mathbb{Z} -lattice N is represented by L but not by M , then*

$$\mu_{k+1}(L) \leq \mu_2(N).$$

Proof. See Lemma 2.4 in [8]. □

Lemma 2.7. *Let L be a \mathbb{Z} -lattice of discriminant D of rank n with the successive minima μ_1, \dots, μ_n . Then there exists a constant $C = C(n)$ such that*

$$D \leq \mu_1 \cdots \mu_n \leq CD.$$

Proof. See Proposition 2.3 in [8]. □

The above lemma implies that if one wants to find an upper bound of the discriminant of a n -ary lattice, then it suffices to find that of the n -th successive minimum, and the converse is also true. This will be used frequently in the following chapters.

2.2 Watson transformation

In this section, we introduce the Watson transformation which makes a lattice into a ‘simpler’ lattice. Taking the Watson transformations to an almost n -regular lattice L , we get an even universal almost n -regular lattice $\lambda(L)$, which is called a terminal lattice of L .

Definition. Let L be a \mathbb{Z} -lattice and let m be a positive integer. Then the lattice

$$\Lambda_m(L) = \{x \in L \mid Q(x+z) \equiv Q(z) \pmod{m} \text{ for all } z \in L\}$$

is called the *Watson transformation* of L modulo m . Let $\lambda_m(L)$ be the even primitive \mathbb{Z} -lattice obtained from $\Lambda_m(L)$ by scaling by a suitable rational number.

The Watson transformation inherits many properties of the original lattice. We gather here some of them. Detailed proofs can be found in [5]. Here, L is an even \mathbb{Z} -lattice and p is a prime number. We suppose that

$$L_p = M_p \perp N_p,$$

where M_p is a leading Jordan component and $\mathfrak{s}(N_p) \subseteq p\mathfrak{s}(M_p)$.

Lemma 2.8. *Suppose that M_p is unimodular and $\mathfrak{n}(N_p) \subseteq 2p\mathbb{Z}_p$. Then*

$$\Lambda_{2p}(L)_p = pM_p \perp N_p.$$

Furthermore, if L is almost n -regular and M_p is anisotropic, then $\lambda_{2p}(L)$ is also almost n -regular.

Lemma 2.9. *If L is almost n -regular and $\mathfrak{s}(L) = 2\mathbb{Z}$, then $\lambda_4(L)$ is also almost n -regular.*

Lemma 2.10. *Suppose that $\mathfrak{s}(L) = 2\mathbb{Z}$ and $\mathfrak{n}(N_2) \subseteq 8\mathbb{Z}_2$.*

CHAPTER 2. PRELIMINARIES

1. If $\text{rank}(M_2) \geq 3$, then $\lambda_4(L)_2$ is split by a unimodular \mathbb{Z}_2 lattice. Actually, this is true when $\mathfrak{s}(N_2) \subseteq 4\mathbb{Z}_2$.
2. If $\text{rank}(M_2) = 2$, then

$$\lambda_4(L)_2 \simeq \begin{cases} M_2^\epsilon \perp N_2^{\frac{1}{2}} & \text{if } \frac{dM}{4} \equiv 1 \pmod{4}, \\ \mathbb{P} \perp N_2^{\frac{1}{4}} & \text{if } \frac{dM}{4} \equiv 3 \pmod{4}, \end{cases}$$

where $\epsilon \in \mathbb{Z}_2^\times$ and \mathbb{P} is an even binary unimodular \mathbb{Z}_2 -lattice.

3. If $\text{rank}(M_2) = 1$, then $\lambda_4(L)_2 \simeq M_2 \perp N_2^{\frac{1}{4}}$.

Lemma 2.11. *If $\text{rank}(M_2) = 1$ and $N_2 = J_2 \perp K_2$ where J_2 is a 4-modular \mathbb{Z}_2 -lattice and $\mathfrak{s}(K_2) \subseteq 8\mathbb{Z}_2$, then*

$$\lambda_4(L)_2 \simeq \begin{cases} M_2^2 \perp N_2^{\frac{1}{2}} & \text{if } \mathfrak{n}(J_2) = \mathfrak{s}(J_2), \\ M_2 \perp N_2^{\frac{1}{4}} & \text{if } \mathfrak{n}(J_2) = 2\mathfrak{s}(J_2). \end{cases}$$

Applying above lemmas to an almost n -regular \mathbb{Z} -lattice for a fixed prime number, one can obtain the following proposition.

Proposition 2.12. *Let L be an even almost n -regular \mathbb{Z} -lattice of rank greater than 4 and let p be a prime number. Then there exists an even almost n -regular \mathbb{Z} -lattice L' satisfying*

$$L'_q \simeq \begin{cases} \mathbb{H} \perp N_p & \text{if } q = p, \\ L_q^{\epsilon_q} & \text{if } q \neq p, \end{cases}$$

where $\mathbb{H} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, N_p is a \mathbb{Z}_p -lattice and $\epsilon_q \in \mathbb{Z}_q^\times$.

Corollary 2.13. *Let L be an even almost n -regular \mathbb{Z} -lattice of rank $m \geq 5$, and suppose that $n \geq 2$. Then there exists an even almost n -regular \mathbb{Z} -lattice $\lambda(L)$ of rank m which is even universal and $d\lambda(L)$ divides dL .*

CHAPTER 2. PRELIMINARIES

Proof. Applying the above proposition for all prime numbers dividing $2dL$, we obtain the desired lattice. The even universality follows from Lemma 2.4. \square

We call the lattice $\lambda(L)$ in the corollary a *terminal lattice* of L . Note that \mathbb{H} is represented by the genus of a terminal lattice.

Next we show that the set of prime divisors of the discriminant of L is ‘bounded’ from that of a terminal lattice of L . For a lattice M , let $P(M)$ be the set of all prime numbers dividing dM .

Proposition 2.14. *Let L be an even almost n -regular \mathbb{Z} -lattice and $\lambda(L)$ be a terminal lattice of L . Then*

$$P(L) \subseteq P(\lambda(L)) \cup \{2, 3, 5, 7, 11, 13\}.$$

Proof. Let p be an odd prime divisor of dL . Applying Proposition 2.12 for all primes $q \neq p$, we can assume that L_q represents all elements in \mathbb{Z}_q . If p does not divide $d\lambda(L)$, one of the followings holds:

- $L_p \simeq \langle a \rangle \perp N_p$ where $a \in \mathbb{Z}_p^\times$ and $s(N_p) \subseteq p^2\mathbb{Z}_p$;
- $L_p \simeq \langle 1, -\Delta_p \rangle \perp N_p$ where $s(N_p) \subseteq p^2\mathbb{Z}_p$.

Here, Δ_p is a non-square unit in \mathbb{Z}_p .

First suppose that $L_p \simeq \langle a \rangle \perp N_p$ and let

$$P = \{2t \mid 1 \leq t \leq p-1, 2t \in Q(L_p)\}.$$

Then $|P| = (p-1)/2$ since p is odd, and $\min(P) \leq p+1$. Let H be the sublattice of L generated by all vectors $v \in L$ such that $Q(v) \in P$. If $\text{rank}(H) = k \geq 3$, then

$$p^{2(k-1)} \leq dH \leq (p+1)(2p-2)^{k-1}$$

CHAPTER 2. PRELIMINARIES

by Lemma 2.7. But this cannot be possible for any odd prime number p . If $\text{rank}(H) = 2$, then

$$dH \leq (p+1)(2p-2).$$

Since H is an even binary lattice, $dH \equiv 0$ or $3 \pmod{4}$. As $p^2 | dH$, this implies that $3p^2 \leq dH$. But $3p^2 \leq 2(p^2-1)$ is not possible. Hence $\text{rank}(H) = 1$ and $|P| \leq \sqrt{p}$. This is possible only when $p \leq 5$.

Next suppose $L_p \simeq \langle 1, -\Delta_p \rangle \perp N_p$. In this case, $\mathbb{Z}_p^\times \subseteq Q(L_p)$ and by Lemma 2.4, L represents all integers in the set $U = \{2, 4, \dots, 2(p-1)\}$. Let G be the sublattice generated by all vectors $v \in L$ such that $Q(v) \in U$. As p is odd, G represents both 2 and 4 and $\text{rank}(G) \geq 2$. If $\text{rank}(G) = k \geq 4$, then

$$p^{2(k-2)} \leq dG \leq 8(2p-2)^{k-2}.$$

This is possible only when $k = 4$ and $p = 3$. If $\text{rank}(G) = 3$,

$$p^2 \leq 8(2p-2)$$

and this holds only when $p \leq 13$. Finally, if G is binary, then G is isometric to one of the followings:

$$[2, 0, 2], [2, 1, 2], [2, 0, 4] \text{ or } [2, 1, 4].$$

Note that these lattices do not represent 6, 4, 10 and 6 respectively. Hence $p \leq 5$. \square

2.3 Analytic tools

In this section, we introduce some analytic results which guarantee the upper bounds of discriminants of almost n -regular lattices. The first proposition is related with the estimation of character sums, which was introduced by Earnest in [8].

Let $\chi_1, \chi_2, \dots, \chi_r$ be Dirichlet characters modulo k_1, k_2, \dots, k_r , respec-

CHAPTER 2. PRELIMINARIES

tively. Let Γ be the least common multiple of k_1, k_2, \dots, k_r , and let $\eta_1, \eta_2, \dots, \eta_r$ (e_1, e_2, \dots, e_r) be elements of $\{1, -1\}$ ($\{1, 2\}$, respectively). Then $\prod_{i=1}^r (\eta_i \chi_i)^{e_i}$ is a Dirichlet character modulo Γ . The characters $\chi_1, \chi_2, \dots, \chi_r$ are said to be *independent* if $\prod_{i=1}^r (\eta_i \chi_i)^{e_i}$ is non-principal whenever $e_i \neq 2$ for some i . For a positive integer H , we put

$$S(H) = \{n < H \mid (n, \Delta) = 1 \text{ and } \chi_i(n) = \eta_i \text{ for all } i\},$$

where Δ is a positive integer relatively prime to Γ . Define

$$h = \min\{H \mid S(H) \neq \emptyset\}.$$

The following Proposition gives an upper bound of h . Here, $A \ll B^{t+\epsilon}$ means that for any $\epsilon > 0$, there exists a constant c which depends only on ϵ satisfying $|A| < cB^{t+\epsilon}$.

Proposition 2.15. *Suppose that the characters $\chi_1, \chi_2, \dots, \chi_r$ are independent and $r \leq \omega(\Gamma) + 1$, where $\omega(\Gamma)$ denotes the number of distinct prime divisors of Γ . Then, for any positive real number $\epsilon > 0$,*

$$h \ll \Gamma^{\frac{3}{8}+\epsilon} \Delta^\epsilon.$$

Proof. See [8]. □

The next result is concerning about the distribution of prime numbers in some arithmetic progression, which was proved by Kozlov [11].

Proposition 2.16. *Let $d \geq 3$ and $\lambda \geq 2$ be integers such that*

$$\sigma := \sum_{\substack{p < d, \\ (p, d) = 1}} \frac{1}{p} < 1$$

and

$$\lambda (1 - \sigma) > 2 + \frac{1}{d-1} \left(1 + \frac{1}{64d^2}\right).$$

CHAPTER 2. PRELIMINARIES

Then, for a real number x such that

$$x \geq \max \{ 64d^4\lambda^2 + 2d, (dk)^2 \},$$

every interval of the form $(x, \lambda x]$ contains at least k primes $p \equiv a \pmod{d}$.

Proof. See [11].

□

Chapter 3

Terminal lattices

In this chapter, we show that terminal lattices of even almost 2-regular quinary lattices are finite up to isometry. In the first section, we define a core lattice which plays a central role in the proof of the finiteness of terminal lattices. In Section 2, we construct a core lattice of a terminal lattice L which is represented by $\text{gen}(L)$ but not by a quaternary section of L to obtain an upper bound of dL .

3.1 Core lattices

Let L be a primitive almost 2-regular quinary lattice. As $\mathbb{Q}L$ is universal, there exists a quaternary space V such that

$$\mathbb{Q}L \simeq \langle dL \rangle \perp V$$

with $dV = 1$.

Lemma 3.1. *There is at least one prime number p such that V_p is anisotropic.*

Proof. Note that if V_p is anisotropic, then

$$V_p \simeq \langle 1, -\Delta_p, p, -p\Delta_p \rangle.$$

CHAPTER 3. TERMINAL LATTICES

Here, Δ_p is a non-square unit in \mathbb{Z}_p if p is odd; otherwise Δ_2 is a unit contained in the square class $5\mathbb{Z}_2^2$. Thus V_p is isotropic if and only if

$$S_p(V) = \begin{cases} 1 & \text{if } p \text{ is odd,} \\ -1 & \text{if } p = 2. \end{cases}$$

Hence the Hilbert Reciprocity Law implies that V_p is anisotropic for at least one prime p . \square

We call the prime number in Lemma 3.1 a *core prime* of L .

Definition. Let R be one of the ring of rational integers \mathbb{Z} or the ring of p -adic integers \mathbb{Z}_p for a prime number p . For an R -lattice L , we call an R -lattice ℓ a *R -core lattice* of L if the failure of L to represent ℓ implies the failure of L to represent infinitely many sublattices of ℓ .

The next lemma shows that a terminal lattice always has a local core lattice.

Lemma 3.2. *Suppose that L is a terminal lattice and p is a core prime of L . Also suppose that $dL_p = p^{\text{ord}_p(dL)}\epsilon_p$, where $\epsilon_p \in \mathbb{Z}_p^\times$. Then L_p has a \mathbb{Z}_p -core lattice of the following form:*

$$\begin{cases} \langle p^{\pi(\text{ord}_p(dL))}\epsilon_p, p^\kappa\eta_p \rangle & \text{if } p \text{ is odd,} \\ \langle 2^{\phi(\text{ord}_2(dL))}\epsilon_2, 2^\kappa\eta_2 \rangle & \text{if } p = 2. \end{cases}$$

Here, η_p is any unit in \mathbb{Z}_p and π, ϕ are functions defined as follow:

$$\pi(n) = \begin{cases} 0 & \text{if } n \text{ is even,} \\ 1 & \text{otherwise} \end{cases}$$

and

$$\phi(n) = \begin{cases} 2 & \text{if } n \text{ is even,} \\ 1 & \text{otherwise.} \end{cases}$$

The exponent κ depends on $\text{ord}_p(dL)$ and is defined in the proof.

CHAPTER 3. TERMINAL LATTICES

Proof. First we suppose that p is odd. If $\text{ord}_p(dL)$ is even, as p is a core prime of L , one can deduce that

$$L_p \simeq \langle 1, -1, p^{2k_1}\epsilon_p\Delta_p, p^{2k_2+1}\delta_p, -p^{2k_3+1}\delta_p\Delta_p \rangle$$

for some unit δ_p in \mathbb{Z}_p and non-negative integers k_1, k_2 and k_3 . Put $\kappa = \max\{2k_1, 2k_2 + 1, 2k_3 + 1\}$. Then

$$\langle \epsilon_p, p^\kappa \eta \rangle$$

is a \mathbb{Z}_p -core lattice of L_p . Here, κ satisfies $\kappa \leq \text{ord}_p(dL) - 1$. Similarly, if $\text{ord}_p(dL)$ is odd, one can show that

$$\langle p\epsilon_p, p^\kappa \rangle$$

is a \mathbb{Z}_p -core lattice of L_p . In this case, $\kappa \leq \text{ord}_p(dL)$.

Suppose that $p = 2$. Since L_2 is even universal, we can consider an orthogonal complement K of $\langle 2^{\phi(\text{ord}_2(dL))}\epsilon_2 \rangle$ in L_2 . Then K is a sublattice of $I_4 = \langle 1, 1, 1, 1 \rangle$ since K is anisotropic. Note that $[I_4 : K] = 2^n$ for a non-negative integer $n \leq \frac{1}{2}(\text{ord}_2(dL) + 2)$. Suppose that $I_4 = \oplus \mathbb{Z}_2 x_i$ and $K = \oplus \mathbb{Z}_2 a_i x_i$ for some $a_i \in \mathbb{Z}_2$. For $j = \max_i \{\text{ord}_2(a_i)\}$, put $a = 2^j$. Then a divides 2^n and $aI_4 \subseteq K$. Therefore

$$2^{\text{ord}_2(dT)+2}\mathbb{Z}_2 \subseteq Q(K).$$

Note that any element in $2^{\text{ord}_2(dT)+5}\mathbb{Z}_2$ cannot be primitively represented by K since any sublattice of I_4 with index 2^d cannot primitively represent any element divided by 2^{2d+3} . Hence the binary lattice

$$\langle 2^{\phi(\text{ord}_2(dL))}\epsilon_2, 2^\kappa \eta_2 \rangle,$$

where $\kappa = \text{ord}_2(dL) + 5$ and η_2 is any unit in \mathbb{Z}_2 , is a \mathbb{Z}_2 -core lattice of L_2 . \square

CHAPTER 3. TERMINAL LATTICES

From a local core lattice, one can construct a global core lattice by the following lemma, which is easily verified by Theorem 2.3.

Lemma 3.3. *Let L be a quinary \mathbb{Z} -lattice and let N be a binary \mathbb{Z} -lattice. Suppose that N_p is a \mathbb{Z}_p -core lattice of L_p for a prime number p . Then N is a \mathbb{Z} -core lattice of L .*

3.2 Finiteness of terminal lattices

In this section, we prove that there are only finitely many primitive terminal lattices up to isometry. Throughout this section, we assume that T is a terminal lattice obtained from an almost 2-regular quinary \mathbb{Z} -lattice. If the 5-th successive minimum $\mu_5(T)$ of T is bounded, then by Lemma 2.7, dT is also bounded. Hence we assume that $\mu_5(T)$ is sufficiently large.

As T is even universal, $\mu_4(T)$ is bounded and there exists an even universal quaternary sublattice M of T . Note that such M are finite by “The 290-Theorem ([1])”. Let S be the set of all primes p such that there is an even universal quaternary \mathbb{Z} -lattice whose discriminant is divisible by p . Clearly, S is a finite set containing 2, 3 and 7. First we handle the case when dM is square.

Proposition 3.4. *Let T be a terminal lattice and M be an even universal quaternary sublattice of T . If dM is square, then the discriminant of T is bounded.*

Proof. Since dM is square, the Hilbert Reciprocity Law implies that M_q is anisotropic for some prime number $q \in S$. Suppose that $S = \{2, q_1, q_2, \dots, q_r\}$, where q_i are odd prime numbers. For a positive integer s , let N_s be a binary lattice given by

$$N_s \simeq \begin{bmatrix} 64q_1^2 \cdots q_r^2 & 1 \\ 1 & 2s \end{bmatrix}.$$

If $p \in S$, then $(N_s)_p \simeq \mathbb{H}$ is represented by T_p ; if $p \notin S$, $M_p \simeq I_4$ which is 2-universal over \mathbb{Z}_p . Hence N_s is represented by $\text{gen}(T)$. Since T is almost

CHAPTER 3. TERMINAL LATTICES

2-regular, T represents N_s for some s . But, for the prime number $q \in S$ such that M_q is anisotropic, $(N_s)_q \simeq \mathbb{H}$ is not represented by M_q . Therefore N_s is not represented by M , and

$$\mu_5(L) \leq 64q_1^2 \cdots q_r^2.$$

Hence Lemma 2.7 leads to the conclusion. \square

Theorem 3.5. *There are only finitely many primitive terminal almost 2-regular quinary \mathbb{Z} -lattices up to isometry.*

Proof. Let T be a terminal almost 2-regular quinary \mathbb{Z} -lattice and let M be an even universal quaternary sublattice of T such that dM is non-square. For each M , choose distinct odd prime numbers q_1, q_2 and q_3 such that

$$M_{q_i} \simeq \langle 1, 1, 1, \Delta_{q_i} \rangle$$

for all i . Since M is even universal, T represents at least one of

$$\langle 2, 2 \rangle, \quad \langle 2, 6 \rangle, \quad \langle 2, 4 \rangle \quad \text{or} \quad \langle 2, 14 \rangle.$$

We define $\beta(T) \in \{2, 4, 6, 14\}$ so that $\langle 2, \beta(T) \rangle$ is represented by T .

Let ℓ be a core prime of T and suppose that $dT = \ell^{\text{ord}_\ell(dT)} u$ with $(u, \ell) = 1$. We can choose two primes among $\{q_1, q_2, q_3\}$ different from ℓ , which we denote q_1 and q_2 after renumbering. Note that they are independent of T and ℓ . Let q be one of q_1, q_2 and suppose that

$$T_q \simeq \langle 1, 1, 1, \Delta_q, q^\omega \epsilon_q \rangle$$

for some $\epsilon_q \in \mathbb{Z}_q^\times$ and a non-negative integer ω . We separate the proof into two steps.

STEP 1 : First inequality

First assume that the core prime ℓ is odd. Note that we can choose an

CHAPTER 3. TERMINAL LATTICES

integer A satisfying

$$\begin{cases} 0 \leq A < q \left(16 \prod_{p \in S - \{2, \ell\}} p \right) \\ q^{\omega + \pi(\omega + 1)} \ell^\kappa A \equiv 2 \pmod{16 \prod_{p \in S - \{2, \ell\}} p}, \\ \ell^\kappa A \equiv 1 \pmod{q}. \end{cases}$$

Recall that π is a function defined as

$$\pi(n) = \begin{cases} 0 & \text{if } n \text{ is even,} \\ 1 & \text{otherwise} \end{cases}.$$

Let P be the product of prime numbers less than $q \left(16 \prod_{p \in S - \{2, \ell\}} p \right)$ that are not contained in $S \cup \{\ell, q\}$. Let B be a positive integer such that

$$\begin{cases} q^{\omega + \pi(\omega + 1)} \ell^{\pi(\text{ord}_\ell(dT))} B \equiv \beta(T) \pmod{32 \cdot 3 \cdot 7 \cdot \prod_{p \in S - \{\ell\}} p}, \\ \left(\frac{\ell^{\pi(\text{ord}_\ell(dT))} B}{q} \right) = - \left(\frac{-1}{q} \right), \\ q^{\omega + \pi(\omega + 1)} \cdot B \equiv u \pmod{\ell}, \\ B \equiv 1 \pmod{P}. \end{cases}$$

By Proposition 2.15, we can choose B so that there is a constant C such that $0 < B < C \cdot \ell^{\frac{1}{2}}$.

Let N be a binary \mathbb{Z} -lattice defined by

$$N = \langle q^{\omega + \pi(\omega + 1)} \ell^\kappa A, q^{\omega + \pi(\omega + 1)} \ell^{\pi(\text{ord}_\ell(dT))} B \rangle, \quad (3.1)$$

where κ is defined as in Lemma 3.2. For any prime $p \in S - \{\ell\}$,

$$N_p \simeq \langle 2, \beta(T) \rangle \rightarrow M_p \rightarrow T_p.$$

Since

$$N_q \simeq \langle q^{\omega + \pi(\omega + 1)}, q^{\omega + \pi(\omega + 1)} (-\Delta_q) \rangle,$$

CHAPTER 3. TERMINAL LATTICES

we have $N \nrightarrow M$ and $N_q \rightarrow T_q$ (See [17]). Furthermore, N_ℓ is a \mathbb{Z}_ℓ -core lattice of T_ℓ . Finally, for any prime $p \notin S \cup \{\ell, q\}$, N_p represents a unit in \mathbb{Z}_p . Hence $N_p \rightarrow M_p \rightarrow T_p$. Therefore, by Lemma 3.3, N is a \mathbb{Z} -core lattice which is represented by the genus of T . This implies that N should be represented by T . Since N is not represented by M ,

$$\mu_5(T) \leq \mu_2(N)$$

by Lemma 2.6. Consequently, there is a constant C_1 such that

$$q^{\text{ord}_q(dT)} \ell^{\text{ord}_\ell(dT)} \leq dT \leq C_1 \cdot q^{\omega + \pi(\omega+1)} \ell^{\max\{\kappa, \pi(\text{ord}_\ell(dT)) + \frac{1}{2}\}}. \quad (3.2)$$

From this, we have

$$\frac{dT}{q^{\text{ord}_q(dT)} \ell^{\text{ord}_\ell(dT)}} \leq C_1 \cdot q \cdot \ell^{\max\{\kappa - \text{ord}_\ell(dT), \pi(\text{ord}_\ell(dT)) - \text{ord}_\ell(dT) + \frac{1}{2}\}} \quad (3.3)$$

Multiplying the inequalities (3.3) obtained from q_1 and q_2 respectively, we get

$$\begin{aligned} \frac{dT}{\ell^{2\text{ord}_\ell(dT)}} &\leq \frac{dT^2}{q_1^{\text{ord}_{q_1}(dT)} q_2^{\text{ord}_{q_2}(dT)} \ell^{2\text{ord}_\ell(dT)}} \\ &\leq C_2 \cdot \ell^{2\max\{\kappa - \text{ord}_\ell(dT), \pi(\text{ord}_\ell(dT)) - \text{ord}_\ell(dT) + \frac{1}{2}\}} \end{aligned}$$

for some constant C_2 independent of T and ℓ . Therefore,

$$dT \leq C_2 \cdot \ell^{3\text{ord}_\ell(dT)} \quad (3.4)$$

Next, suppose that $\ell = 2$. Recall that $\kappa = \text{ord}_2(dT) + 5$ in this case. Let P be the product of prime numbers less than $q(\prod_{p \in S - \{2\}} p)$ that are not

CHAPTER 3. TERMINAL LATTICES

contained in $S \cup \{q\}$. Choose integers A and B satisfying

$$\begin{cases} 0 \leq A < q(\prod_{p \in S - \{2\}} p), \\ q^{\omega + \pi(\omega + 1)} 2^\kappa A \equiv 2 \pmod{\prod_{p \in S - \{2\}} p}, \\ 2^\kappa A \equiv 1 \pmod{q} \end{cases}$$

and

$$\begin{cases} q^{\omega + \pi(\omega + 1)} 2^{\phi(\text{ord}_2(dT))} B \equiv \beta(T) \pmod{3 \cdot 7 \cdot \prod_{p \in S - \{2\}} p}, \\ q^{\omega + \pi(\omega + 1)} B \equiv u \pmod{8}, \\ B \equiv 1 \pmod{P}, \\ \left(\frac{2^{\phi(\text{ord}_2(dT))} B}{q} \right) = - \left(\frac{-1}{q} \right). \end{cases}$$

Recall that ϕ is defined as

$$\phi(n) = \begin{cases} 2 & \text{if } n \text{ is even,} \\ 1 & \text{otherwise} \end{cases},$$

and note that B is bounded in this case.

Let N be a binary \mathbb{Z} -lattice defined by

$$N = \langle q^{\omega + \pi(\omega + 1)} 2^\kappa A, q^{\omega + \pi(\omega + 1)} 2^{\phi(\text{ord}_2(dT))} B \rangle. \quad (3.5)$$

Then, as above, N is represented by T but not by M , and we get the following inequality

$$dT \leq C \cdot 2^{\text{ord}_2(dT)} \quad (3.6)$$

for some constant C independent of T and ℓ .

STEP 2 : Second inequality

To find an upper bound of the discriminant of T , it suffices to show that $\ell^{\text{ord}_\ell(dT)}$ is bounded by the inequalities (3.4) and (3.6). Since all the

CHAPTER 3. TERMINAL LATTICES

other cases can be done in a similar manner, we only consider the case when $\beta(T) = 6$.

Suppose that ℓ is odd. From the inequality (3.2), we see that $\ell^{\text{ord}_\ell(dT)-\kappa}$ is bounded. If $\ell^{\text{ord}_\ell(dT)}$ is bounded, clearly dT is bounded. Hence we assume that ℓ^κ is sufficiently large. Choose a prime p such that

$$[\ell^{\frac{8}{23}\kappa}] \leq p < 7[\ell^{\frac{8}{23}\kappa}]$$

and

$$\begin{cases} p \equiv q \pmod{3} & \text{if } \kappa \text{ is even,} \\ p \equiv \ell \cdot q \pmod{3} & \text{if } \kappa \text{ is odd,} \end{cases}$$

which is possible by Proposition 2.16. First suppose that $\text{ord}_\ell(dT)$ is even. Define a positive integer A such that

$$\begin{cases} \left(\frac{A}{r}\right) = \left(\frac{\ell^\kappa}{r}\right) & \text{for any } r \in S - \{2\}, \\ A \equiv \ell^\kappa \pmod{8}, \\ \left(\frac{A}{q}\right) = -\left(\frac{-3\ell^\kappa}{q}\right), \\ \left(\frac{A}{p}\right) = \left(\frac{-3\ell^\kappa}{p}\right), \\ \left(\frac{A}{\ell}\right) = \left(\frac{2pqu}{\ell}\right). \end{cases}$$

Note that by Proposition 2.15, for any $\epsilon > 0$, we may choose A satisfying $A \ll (p\ell)^{\frac{3}{8}+\epsilon}$.

Since $\left(\frac{A}{p}\right) = \left(\frac{-3\ell^\kappa}{p}\right)$, there is an integer k ($1 \leq k \leq p-1$) such that $3A\ell^\kappa + k^2$ is divisible by p . Let $pv - k^2 = 3A\ell^\kappa$ and define a binary \mathbb{Z} -lattice N by

$$N \simeq q^{\omega+\pi(\omega+1)} A \begin{pmatrix} 2p & 2k \\ 2k & 2v \end{pmatrix}.$$

Note that $dN = 12A^3\ell^\kappa q^{2(\omega+\pi(\omega+1))}$. Then

CHAPTER 3. TERMINAL LATTICES

- (i) since $dN_r = 3$ for any $r \in S - \{2, 3\}$, we have $N_r \simeq \langle 2, 6 \rangle \rightarrow M_r \rightarrow T_r$;
- (ii) since every binary odd unimodular \mathbb{Z}_2 -lattice with discriminant 3 is isometric to $\langle 1, 3 \rangle$, we have $N_2 \simeq \langle 2, 6 \rangle \rightarrow M_2 \rightarrow T_2$;
- (iii) since $dN_3 = 3$, $N_3 \simeq \langle 2pqA, 6pqA \rangle$; if κ is even, $A \sim pq \sim 1$; otherwise, $A \sim \ell$ and $pq\ell \sim 1$. Hence $N_3 \simeq \langle 2, 6 \rangle \rightarrow M_3 \rightarrow T_3$;
- (iv) since $N_q \simeq \langle q^{\omega+\pi(\omega+1)}, (-\Delta_q)q^{\omega+\pi(\omega+1)} \rangle$, $N_q \not\rightarrow M_q$ and $N_q \rightarrow T_q$;
- (v) both N_p and M_p are unimodular \mathbb{Z}_p -lattices;
- (vi) since $N_\ell \simeq \langle 2pqA, 6pq\ell^\kappa \rangle \simeq \langle u, \ell^\kappa \eta \rangle$ ($\eta \in \mathbb{Z}_\ell^\times$), N_ℓ is a binary \mathbb{Z}_ℓ -core lattice of T_ℓ ;
- (vii) for any prime $r \notin S \cup \{\ell, q, p\}$, $N_r \simeq \langle 2pqA, 6pqA^2\ell^\kappa \rangle$ is not isometric to $\langle r^{2s+1}\epsilon_r, -r^{2t+1}\epsilon_r\Delta_r \rangle$ for any unit $\epsilon_r \in \mathbb{Z}_r$ and integers r, s , and hence $N_r \rightarrow M_r$.

Here, we use the notation $a \sim b$ to denote that a and b are units in the same square class. Therefore N is represented by T but not by M , and we have

$$q^{\text{ord}_q(dT)} \ell^{\text{ord}_\ell(dT)} \leq dT \leq C_1 \cdot q^{\omega+\pi(\omega+1)} \max\{pA, vA\}, \quad (3.7)$$

for some constant C_1 independent of T and ℓ . Now choose ϵ so small that $\epsilon < \frac{1}{16}$. Since $p \ll \ell^{\frac{8}{23}\kappa}$, $A \ll (p\ell)^{\frac{3}{8}+\epsilon} \ll \ell^{\frac{7}{46}\kappa+\frac{7}{16}}$. Hence $pA \ll \ell^{\frac{1}{2}\kappa+\frac{7}{16}}$ and

$$vA \ll \max\left\{\frac{A^2\ell^\kappa}{p}, \frac{Ak^2}{p}\right\} \ll \max\left\{\ell^{\frac{22}{23}\kappa+\frac{7}{8}}, \ell^{\frac{1}{2}\kappa+\frac{7}{16}}\right\} \ll \ell^{\frac{22}{23}\kappa+\frac{7}{8}}. \quad (3.8)$$

Combining (3.7) and (3.8), we get

$$\ell^{\text{ord}_\ell(dT)} < C_2 \cdot \ell^{\frac{22}{23}\text{ord}_\ell(dT)+\frac{7}{8}}.$$

Therefore $\ell^{\text{ord}_\ell(dT)}$ is bounded by an absolute constant.

CHAPTER 3. TERMINAL LATTICES

Next suppose that $\text{ord}_\ell(dT)$ is odd. Define a positive integer A such that

$$\left\{ \begin{array}{l} \left(\frac{A}{r} \right) = \left(\frac{\ell^{\kappa-1}}{r} \right) \quad \text{for any } r \in S - \{2\}, \\ A \equiv \ell^{\kappa-1} \pmod{8}, \\ \left(\frac{A}{q} \right) = - \left(\frac{-3\ell^{\kappa-1}}{q} \right), \\ \left(\frac{A}{p} \right) = \left(\frac{-3\ell^{\kappa-1}}{p} \right), \\ \left(\frac{A}{\ell} \right) = \left(\frac{2pqu}{\ell} \right). \end{array} \right.$$

As before, we choose A satisfying $A \ll (p\ell)^{\frac{3}{8}+\epsilon}$.

Since $\left(\frac{A}{p} \right) = \left(\frac{-3\ell^{\kappa-1}}{p} \right)$, there is an integer k ($1 \leq k \leq p-1$) such that $3A\ell^{\kappa-1} + k^2$ is divisible by p . Let $pv - k^2 = 3A\ell^{\kappa-1}$ and define a binary \mathbb{Z} -lattice N by

$$N \simeq q^{\omega+\pi(\omega+1)} A\ell \begin{pmatrix} 2p & 2k \\ 2k & 2v \end{pmatrix}.$$

Note that $dN = 12A^3\ell^{\kappa+1}q^{2(\omega+\pi(\omega+1))}$. Then $N_\ell \simeq \langle \ell u, \ell^\kappa \eta \rangle$ and N is represented by T but not by M . Also $pA\ell \ll \ell^{\frac{1}{2}\kappa + \frac{23}{16}}$ and $vA\ell \ll \ell^{\frac{22}{23}\kappa + \frac{7}{8}}$. Therefore $\ell^{\text{ord}_\ell(dT)}$ is bounded.

Now suppose that $\ell = 2$ and $\text{ord}_2(dT)$ is sufficiently large. Then we can choose a prime p such that

$$[2^{\frac{8}{23}\kappa}] \leq p < 7[2^{\frac{8}{23}\kappa}]$$

and

$$\begin{cases} p \equiv q \pmod{3} & \text{if } \text{ord}_2(dT) \text{ is odd,} \\ p \equiv 2q \pmod{3} & \text{if } \text{ord}_2(dT) \text{ is even.} \end{cases}$$

CHAPTER 3. TERMINAL LATTICES

Choose a positive integer A satisfying

$$\begin{cases} \left(\frac{A}{r}\right) = 1 & \text{for any } r \in S - \{2\}, \\ A \equiv pqu \pmod{8}, \\ \left(\frac{A}{q}\right) = -\left(\frac{-3}{q}\right), \\ \left(\frac{A}{p}\right) = \left(\frac{-3}{p}\right). \end{cases}$$

Note that $A \ll p^{\frac{3}{8}+\epsilon}$.

First suppose that $\text{ord}_2(dT)$ is even. Since κ is odd, there exists an integer k ($0 \leq k \leq p-1$) such that

$$pv = 3 \cdot A \cdot 2^{\kappa-1} + k^2.$$

Define a binary \mathbb{Z} -lattice N by

$$N \simeq q^{\omega+\pi(\omega+1)} 2A \begin{pmatrix} 2p & 2k \\ 2k & 2v \end{pmatrix}.$$

Then $dN = 3 \cdot 2^{\kappa+3} \cdot A^3 \cdot q^{2(\omega+\pi(\omega+1))}$. Note that

- (i) for $r \in S - \{2, 3\}$, $dN_r = 3$ and $N_r \simeq \langle 2, 6 \rangle \rightarrow M_r \rightarrow T_r$;
- (ii) for $r = 2$, $N_2 \simeq \langle 4pqA, 3 \cdot 2^{\kappa+1}pqA^2 \rangle \simeq \langle 4u, 2^{\kappa+1}\eta \rangle$, which is a \mathbb{Z}_2 -core lattice of T_2 ;
- (iii) for $r = 3$, $dN_3 = 3$ and $N_3 \simeq \langle pqA, 3pgA \rangle \simeq \langle 2, 6 \rangle \rightarrow M_r \rightarrow T_r$;
- (iv) for $r = q$, $N_q \simeq \langle q^{2(\omega+\pi(\omega+1))}, (-\Delta_q)q^{2(\omega+\pi(\omega+1))} \rangle$, which is represented by T_q but not by M_q ;
- (v) for $r = p$, N_p and M_p are unimodular and $N_p \rightarrow M_p \rightarrow T_p$;
- (vi) for $r \notin S \cup \{p, q\}$, $N_r \simeq \langle pqA, 3pqA^2 \rangle \not\simeq \langle r^{2s+1}\epsilon_r, -r^{2t+1}\epsilon_r\Delta_r \rangle$ and hence $N_r \rightarrow M_r \rightarrow T_r$.

CHAPTER 3. TERMINAL LATTICES

Therefore there exists a constant C such that

$$dT \leq C \cdot q^{\omega+\pi(\omega+1)} \max\{pA, vA\}.$$

Choose ϵ so small that $\epsilon < \frac{1}{16}$. Then $p \ll 2^{\frac{8}{23}\kappa}$ and $A \ll 2^{\frac{7}{46}\kappa}$. Hence $pA \ll 2^{\frac{1}{2}\kappa}$ and

$$vA \ll \max\left\{\frac{A^2 2^{\kappa-1}}{p}, \frac{Ak^2}{p}\right\} \ll \max\{2^{\frac{22}{23}\kappa-1}, 2^{\frac{1}{2}\kappa}\} < 2^{\frac{22}{23}\kappa}.$$

Therefore we have

$$q^{\text{ord}_q(dT)} 2^{\text{ord}_2(dT)} \leq dT \leq C_1 \cdot q^{\omega+\pi(\omega+1)} 2^{\frac{22}{23}\kappa}$$

for some constant C_1 and hence dT is bounded.

Next suppose that $\text{ord}_2(dT)$ is odd. Let k be an integer such that $0 \leq k \leq p-1$ and $pv = 3 \cdot A \cdot 2^\kappa + k^2$. Define a binary \mathbb{Z} -lattice N by

$$N \simeq q^{\omega+\pi(\omega+1)} A \begin{pmatrix} 2p & 2k \\ 2k & 2v \end{pmatrix}.$$

Then $dN = 3 \cdot 2^{\kappa+2} \cdot A^3 \cdot q^{2(\omega+\pi(\omega+1))}$, and as above, N is represented by T but not by M . Also

$$q^{\text{ord}_q(dT)} 2^{\text{ord}_2(dT)} \leq dT \leq C_1 \cdot q^{\omega+\pi(\omega+1)} 2^{\frac{22}{23}\kappa}.$$

This completes the proof. □

Chapter 4

Almost 2-regular quinary lattices

In this chapter, we discuss the finiteness of general even almost 2-regular quinary \mathbb{Z} -lattices L . In Section 1, we introduce some reduction results to show that even universal almost 2-regular quinary \mathbb{Z} -lattices are finite up to isometry. In Section 2, we first show that $\text{ord}_p(dL)$ is bounded if p is an odd prime. Next, we prove $\text{ord}_2(dL)$ is bounded if L has an odd core prime. Finally, we explain the remaining problem to complete the proof of the finiteness of even almost 2-regular quinary \mathbb{Z} -lattices.

4.1 Even universal almost 2-regular quinary \mathbb{Z} -lattices

Let L be an even almost 2-regular quinary \mathbb{Z} -lattice. As L is 1-regular, the third successive minimum μ_3 of L is bounded (for example, [4] Corollary 3.2). Since we have shown that terminal lattices are finite up to isometry, Proposition 2.14 implies that the set S of prime divisors of even almost 2-regular quinary lattices is finite. Hence it suffices to fix a prime number p and show that $\text{ord}_p(dL)$ is bounded. Furthermore, after taking λ_{2q} for all

CHAPTER 4. ALMOST 2-REGULAR QUINARY LATTICES

prime numbers $q \neq p$ dividing $2dL$, we can assume that the even unimodular isotropic binary lattice \mathbb{H} is represented by L_q for all prime numbers $q \neq p$ since $\text{ord}_p(dL) = \text{ord}_p(d\lambda_{2q}(L))$.

Lemma 4.1. *Let L be an even almost 2-regular quinary lattice. Suppose that $\mu_4(L)$ is bounded by an absolute constant. Then $\text{ord}_p(dL)$ is bounded.*

Proof. As $\mu_4(L)$ is bounded, taking λ_{2p} bounded times we can assume that \mathbb{H} is represented by L_p , or

$$L_p \simeq \mathbb{A} \perp \mathbb{A}^p \perp \langle p^\alpha \epsilon_p \rangle$$

for a unit $\epsilon_p \in \mathbb{Z}_p$ and a positive integer α . Here, \mathbb{A} is the even unimodular anisotropic binary \mathbb{Z}_p -lattice. If \mathbb{H} is represented by L_p , L itself is a terminal lattice and dL is bounded by Theorem 3.5. Hence suppose that the latter holds and α is sufficiently large. Since L is even universal, there exists an even universal quaternary sublattice M of L . In this case,

$$M_p \simeq \mathbb{A} \perp \mathbb{A}^p,$$

and p is a core prime of L .

First suppose that p is an odd prime. Choose a prime number r such that

$$r \in -(\mathbb{Z}_q^\times)^2 \quad \text{for all prime numbers } q \text{ dividing } 2dL.$$

Also choose a prime number $t > 2p^2r$ such that

$$\begin{cases} t \equiv 2\epsilon_p \pmod{p}, \\ t \equiv 1 \pmod{8}, \\ t \in (\mathbb{Z}_q^\times)^2 \quad \text{for } q \in \{2, r\}. \end{cases}$$

Note that r and t are independent of L and α . Then $\left(\frac{-r}{t}\right) = 1$ and there

CHAPTER 4. ALMOST 2-REGULAR QUINARY LATTICES

exist positive integers k ($< t$) and v such that

$$tv = k^2 + p^{\alpha+\pi(\alpha)}r.$$

Let N be a \mathbb{Z} -lattice defined by

$$N \simeq 2p^{\pi(\alpha)} \begin{pmatrix} t & k \\ k & v \end{pmatrix}.$$

Then

- (i) $N_p \simeq \langle p^{\pi(\alpha)}\epsilon_p, -p^{2\pi(\alpha)+\alpha}\epsilon_p \rangle$, which is an isotropic core lattice of L_p ;
- (ii) $N_q \rightarrow \mathbb{H} \rightarrow L_q$ for all prime numbers $q|2dL$, $q \neq p$;
- (iii) $N_q \rightarrow L_q$ for all prime numbers $q \nmid 2dL$ since L_q is 2-universal.

Therefore N is represented by L but not by M . Then

$$p^\alpha \leq \mu_5(L) \leq 2p^{\pi(\alpha)} \max\{t, v\}.$$

If $v \leq t$, α is bounded by an absolute constant. Hence we assume that

$$p^\alpha \leq 2p^{\pi(\alpha)}v.$$

Then

$$\frac{p^\alpha t}{2p^{\pi(\alpha)}} \leq tv \leq t^2 + p^{\alpha+\pi(\alpha)}r.$$

Therefore we have

$$p^\alpha \leq \frac{2p^{\pi(\alpha)}t^2}{t - 2p^{2\pi(\alpha)}r},$$

and α is bounded.

Next suppose that $p = 2$. Choose a prime number r such that

$$r \in -(\mathbb{Z}_q^\times)^2 \text{ for all prime numbers } q \text{ dividing } 2dL.$$

CHAPTER 4. ALMOST 2-REGULAR QUINARY LATTICES

Also choose a prime number s not dividing $2dL$ such that

$$s \equiv \epsilon_2 \pmod{8}.$$

Finally choose a prime number $t > 2^{10}rs$ such that

$$\begin{cases} t \equiv 1 \pmod{8}, \\ t \in (\mathbb{Z}_r^\times)^2. \end{cases}$$

Note that r, s and t are independent of L and α . As above, there exist positive integers k ($< t$) and v such that

$$tv = k^2 + 2^{\alpha+\phi(\alpha)+6}r.$$

Define a \mathbb{Z} -lattice N by

$$N \simeq 2^{\phi(\alpha)}s \begin{pmatrix} t & k \\ k & v \end{pmatrix}.$$

Then N is represented by L but not by M , and, as above, we have

$$2^\alpha \leq \frac{2^{\phi(\alpha)}st^2}{t - 2^{2\phi(\alpha)+6}rs}.$$

This completes the proof. □

The above lemma implies the finiteness of even universal almost 2-regular quinary \mathbb{Z} -lattices.

Corollary 4.2. *There are only finitely many even almost 2-regular quinary \mathbb{Z} -lattices which represent all even integers up to isometry.*

4.2 Finiteness of even almost 2-regular quinary \mathbb{Z} -lattices

Let L be an even almost 2-regular quinary \mathbb{Z} -lattice. By Corollary 4.2, we may assume that L is not even universal. In this section, we prove that $\text{ord}_p(dL)$ is bounded for any odd prime number p , and discuss what happens if $p = 2$.

Proposition 4.3. *Let L be an even almost 2-regular quinary \mathbb{Z} -lattice and let p be an odd prime divisor of dL . Then $\text{ord}_p(dL)$ is bounded.*

Proof. Since $\mu_3(L)$ is bounded, we take λ_p bounded times to L and assume that

$$\mathbb{H} \rightarrow L_p \quad \text{or} \quad \langle 1, -\Delta_p, p\epsilon_p \rangle \rightarrow L_p,$$

where ϵ_p is a unit in \mathbb{Z}_p . If the former case holds, dL is bounded by Corollary 4.2. Hence we assume that

$$\begin{cases} \mathbb{H} \rightarrow L_q \text{ for all prime numbers } q \neq p, \\ L_p \simeq \langle 1, -\Delta_p, p\epsilon_1, p^\alpha\epsilon_2, p^\beta\epsilon_3 \rangle. \end{cases}$$

Here, ϵ_i are units in \mathbb{Z}_p and $\alpha \leq \beta$ are positive integers. Furthermore, by Lemma 4.1, we assume that α is sufficiently large.

Let G be a ternary section of L . As $\mu_3(L)$ is bounded, such G are finite up to isometry. We claim that there exists an even integer a_G not represented by G such that $a_G \notin p\epsilon_1\Delta_p\mathbb{Z}_p^2$. Suppose that G represents all even integers but integers contained in the square class $p\epsilon_1\Delta_p\mathbb{Z}_p^2$. Then G_q is even universal over \mathbb{Z}_q for all prime numbers $q \neq p$. Since G_q is even universal over \mathbb{Z}_q if and only if \mathbb{H} splits G_q , we have

$$G_q \simeq \mathbb{H} \perp \langle a_q \rangle$$

CHAPTER 4. ALMOST 2-REGULAR QUINARY LATTICES

for some element $a_q \in \mathbb{Z}_q$. Also, the hypothesis implies that

$$G_p \simeq \langle 1, -\Delta_p, p\epsilon_1 \rangle.$$

Then $S_q(\mathbb{Q}G) = 1$ for $q \neq p$ and $S_p(\mathbb{Q}G) = -1$, which contradicts the Hilbert Reciprocity Law. Therefore there exists such an integer a_G . Since the possible choices of a ternary section G and the unit ϵ_1 are finite, we can assume that a_G is independent of L . But, as L is 1-regular, a_G is represented by L . Therefore

$$\mu_4(L) \leq a_G,$$

and Lemma 4.1 shows that $\text{ord}_p(dL)$ is bounded. \square

Finally it remains for us to show that $\text{ord}_2(dL)$ is finite. Since $\mu_3(L)$ is bounded, taking $\lambda_4(L)$ bounded times, L_2 falls into one of the following cases:

$$\mathbb{H} \rightarrow L_2, \quad \mathbb{A} \perp \mathbb{A}^2 \rightarrow L_2 \quad \text{or} \quad \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp \langle 4\epsilon_2 \rangle \rightarrow L_2,$$

where ϵ_2 is a unit in \mathbb{Z}_2 . Since the former two cases are already considered, we assume that L satisfies

$$\begin{cases} \mathbb{H} \rightarrow L_q \text{ for all prime numbers } q \neq 2, \\ L_2 \simeq \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp \langle 4\epsilon_2 \rangle \perp K_2 \end{cases}$$

for some binary \mathbb{Z}_2 -lattice K_2 with $\mathfrak{s}K_2 \subseteq 8\mathbb{Z}_2$. Note that

$$Q \left(\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp \langle 4\epsilon_2 \rangle \right) = 2\mathbb{Z}_2 - 4\Delta_2\epsilon_2\mathbb{Z}_2^2.$$

Suppose that G is a ternary section of L . Note that the choice of such G is finite. If G does not represent an even integer contained in any square

CHAPTER 4. ALMOST 2-REGULAR QUINARY LATTICES

classes of $2\mathbb{Z}_2$ different from $4\Delta_2\epsilon_2\mathbb{Z}_2^2$, then $\mu_4(L)$ is bounded as in the proof of Proposition 4.3. Therefore we assume that G represents all even integers except integers contained in the square class $4\Delta_2\epsilon_2\mathbb{Z}_2^2$. Then G satisfies the local conditions

$$\begin{cases} \mathbb{H} \rightarrow G_q \text{ for all prime numbers } q \neq 2, \\ G_2 \simeq \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp \langle 4\epsilon_2 \rangle. \end{cases} \quad (4.1)$$

Furthermore, if G is not regular, $\mu_4(L)$ is bounded above by an exceptional integer of G which is independent of L . Using the escalation method, one can find all even regular ternary lattices satisfying the above conditions as follows.

Lemma 4.4. *Suppose that G is an even regular ternary \mathbb{Z} -lattice satisfying the above local conditions (4.1). Then G is isometric to one of the following lattices.*

(1) $\epsilon_2 = 1$

$$\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp \langle 4 \rangle \quad \text{or} \quad \begin{pmatrix} 2 & 1 \\ 1 & 6 \end{pmatrix} \perp \langle 4 \rangle;$$

(2) $\epsilon_2 = 3$

$$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 2 & 0 & 1 \\ 0 & 4 & 2 \\ 1 & 2 & 6 \end{pmatrix};$$

(3) $\epsilon_2 = 5$

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 10 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 & 1 \\ 1 & 6 & 1 \\ 1 & 1 & 6 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 2 & 1 & 1 \\ 1 & 6 & 3 \\ 1 & 3 & 10 \end{pmatrix};$$

CHAPTER 4. ALMOST 2-REGULAR QUINARY LATTICES

$$(4) \quad \epsilon_2 = 7$$

$$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 6 \end{pmatrix}.$$

Proposition 4.5. *Let L be an even almost 2-regular quinary lattice. If L has an odd core prime ℓ , then $\text{ord}_2(dL)$ is bounded.*

Proof. We assume that L has a ternary section G isometric to one of the lattices given in Lemma 4.4. Then G contains one of the three diagonal lattices:

$$\langle 2, 2 \rangle, \quad \langle 2, 4 \rangle \quad \text{or} \quad \langle 2, 10 \rangle.$$

Define $\alpha(G) \in \{2, 4, 10\}$ so that $\langle 2, \alpha(G) \rangle \rightarrow G$.

Suppose that $dL = \ell^{\text{ord}_\ell(dL)} u$ with $(u, \ell) = 1$. Here, $\text{ord}_\ell(dL)$ is bounded by Proposition 4.3. Recall that

$$\langle \ell^{\pi(\text{ord}_\ell(dL))} u, \ell^\kappa \eta_\ell \rangle$$

is a \mathbb{Z}_ℓ -core lattice of L_ℓ for any unit η_ℓ in \mathbb{Z}_ℓ . Next, choose a large prime number p not dividing $dG \cdot dL$. Then L_p is 2-universal and

$$G_p \simeq \langle 1, 1, \delta_p \rangle$$

for some unit $\delta_p \in \mathbb{Z}_p^\times$. Hence the \mathbb{Z}_p -lattice

$$\langle p, -\delta_p \Delta_p \rangle$$

is represented by L_p but not by G_p .

Choose positive integers A and B satisfying

$$\begin{cases} A \equiv u \pmod{\ell}, \\ A \equiv \ell^{\pi(\text{ord}_\ell(dL))} \pmod{p}, \\ A \equiv 2\ell^{\pi(\text{ord}_\ell(dL))} p \pmod{16 \cdot \prod_{q \in S - \{\ell\}} q}, \end{cases}$$

CHAPTER 4. ALMOST 2-REGULAR QUINARY LATTICES

and

$$\begin{cases} B \equiv 1 \pmod{\ell}, \\ B \equiv -\ell^\kappa \delta_p \Delta_p \pmod{p}, \\ B \equiv 2\ell^\kappa \alpha(G) \pmod{32 \cdot 5 \cdot \prod_{q \in S - \{\ell\}} q}. \end{cases}$$

Clearly, A and B are bounded.

Let N be a \mathbb{Z} -lattice defined by

$$N \simeq \langle \ell^{\pi(\text{ord}_\ell(dL))} pA, \ell^\kappa B \rangle. \quad (4.2)$$

Then N is represented by L but not by G . Therefore

$$\mu_4(L) \leq \max\{ \ell^{\pi(\text{ord}_\ell(dL))} pA, \ell^\kappa B \}.$$

Since the right side is bounded by an absolute constant, $\text{ord}_2(dL)$ is bounded by Lemma 4.1. \square

Summing up our results obtained so far, we have the following theorem.

Theorem 4.6. (i) *The set of prime divisors of the discriminants of even almost 2-regular quinary \mathbb{Z} -lattices is finite.*

(ii) *There exist only finitely many even primitive almost 2-regular quinary \mathbb{Z} -lattices which have an odd core prime.*

(iii) *There exist only finitely many even primitive almost 2-regular quinary \mathbb{Z} -lattices L if $\text{ord}_2(dL)$ is fixed.*

Remark 4.7. To prove the finiteness of even almost 2-regular quinary \mathbb{Z} -lattices, the only one case is remained: an even almost 2-regular quinary

CHAPTER 4. ALMOST 2-REGULAR QUINARY LATTICES

\mathbb{Z} -lattice L has a unique core prime 2, and satisfies that

$$\left\{ \begin{array}{l} \mathbb{H} \rightarrow L_q \text{ for all prime numbers } q \neq 2, \\ L_2 \simeq \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp \langle 4\epsilon_2 \rangle \perp K_2, \text{ where } \mathfrak{s}K_2 \subseteq 8\mathbb{Z}_2, \\ L \text{ has a ternary section } G \text{ isometric to one in Lemma 4.4.} \end{array} \right.$$

Note that if the scale of K_2 is fixed, such lattices are finite up to isometry. We expect that even almost 2-regular quinary lattices satisfying the above conditions become rarer as $\mathfrak{s}K_2$ grows larger.

Bibliography

- [1] M. Bhargava and J. Hanke, *Universal quadratic forms and the 290-Theorem*, Invent. Math., to appear.
- [2] J. Bochnak and B.-K. Oh, *Almost regular quaternary quadratic forms*, Ann. Inst. Fourier (Grenoble) **58** (2008), 1499–1549.
- [3] J. K. S. Cassels, *Rational quadratic forms*, Academic Press, 1978.
- [4] W. K. Chan, A. G. Earnest and B.-K. Oh, *Regularity properties of positive definite integral quadratic forms*, Contemp. Math., **344** (2004), 59–71.
- [5] W. K. Chan and B.-K. Oh, *Finiteness theorems for positive definite n -regular quadratic forms*, Trans. Amer. Math. Soc., **355** (2003), 2385–2396.
- [6] W. K. Chan and B.-K. Oh, *Positive ternary quadratic forms with finitely many exceptions*, Proc. Amer. Math. Soc., **132** (2004), 1567–1573.
- [7] L. E. Dickson, *Ternary quadratic forms and congruences*, Ann. of Math., **28** (1927), 333–341.
- [8] A. G. Earnest, *The representation of binary quadratic forms by positive definite quaternary quadratic forms*, Trans. Amer. Math. Soc., **345** (1994), 853–863.

BIBLIOGRAPHY

- [9] W. C. Jagy, I. Kaplansky, A. Schiemann, *There are 913 regular ternary forms*, *Mathematika*, **44** (1997), 332–341.
- [10] Y. Kitaoka, *Arithmetic of quadratic forms*, Cambridge University Press, 1993.
- [11] I. M. Kozlov, *On the distribution of prime numbers in some arithmetic progression*, *Moscow Univ. Math. Bull.*, **57** (2002), 30–34.
- [12] B.-K. Oh, *Positive definite n -regular quadratic forms*, *Invent. Math.* **170** (2007), 421–453.
- [13] B.-K. Oh, *Regular positive ternary quadratic forms*, *Acta Arith.*, **147** (2011), 233–243.
- [14] B.-K. Oh, *The representation of quadratic forms by almost universal forms of higher rank*, *Math. Z.*, **244** (2003), 399–413.
- [15] R. J. L. Oliver, *Representation by ternary quadratic forms*, *Bull. Lond. Math. Soc.*, **46** (2014), 1237–1247.
- [16] O. T. O’Meara, *Introduction to quadratic forms*, Springer-Verlag, 1973.
- [17] O. T. O’Meara, *The integral representations of quadratic forms over local fields*, *Amer. J. Math.*, **80** (1958), 843–878.
- [18] G. L. Watson, *Some problems in the theory of numbers*, Ph.D. Thesis, University of London, 1953.
- [19] G. L. Watson, *The representation of integers by positive ternary quadratic forms*, *Mathematika*, **1** (1954), 104–110.
- [20] G. L. Watson, *Regular positive ternary quadratic forms*, *J. London Math. Soc.*, **13** (1976), 97–102.

국문초록

양의 정부호를 가진 정수계수 이차형식이 주어져 있을 때, 그 이차형식이 국소적으로 표현하는 변수가 n 개인 이차형식 중 유한개를 제외하고 대역적으로 모두 표현하는 경우, 이를 거의 모든 n -정규 이차형식이라고 한다.

이 논문에서 우리는 거의 모든 2-정규 5변수 이차형식의 유한성에 대하여 연구한다. 먼저 모든 정수를 표현하는 거의 모든 2-정규 5변수 이차형식이 유한함을 증명한다. 그리고 홀수 핵심 소수를 가지는 거의 모든 2-정규 5변수 이차형식이 유한함을 증명한다. 마지막으로, 2를 유일한 핵심 소수로 가지는 거의 모든 2-정규 5변수 이차형식의 유한성에 대하여 논의한다.

주요어휘: 이차형식, 거의 모든 n -정규 형식, 표현, 왓슨 변환
학번: 2009-22893